BHES

Online Safety Policy

Note: in this policy reference to governing body or governors refers to the management committee and its members.

Where contextually appropriate for school read service.

Date adopted: July 2025

Review **schedule – annually**

HISTORY OF POLICY CHANGES

Date	Page	Details of Change

Contents

1. Introduction

Bristol Hospital Education Service (BHES) provides education to children and young people who are unable to attend mainstream school due to medical, psychological, or emotional needs. This includes:
- Students with physical or mental health conditions
- Emotionally Based School Avoidance (EBSA)
- Pupils receiving 1:1 tuition at home or in the community
- Students attending our base, a Pupil Referral Unit (PRU)

These students are often more vulnerable to online risks due to isolation, reduced peer interaction, and increased screen time. This policy outlines our approach to ensuring their safety in digital environments.

2. Aims

- To protect students from online harm, including grooming, radicalisation, cyberbullying, and exposure to inappropriate content.
- To educate students, staff, and families about safe and responsible use of technology.
- To ensure robust safeguarding procedures are in place for all digital interactions.

3. Key Online Risks

3.1 Student-Specific Risks
- Isolation: Students learning alone may seek connection online, increasing vulnerability to exploitation.
- Mental Health: Anxiety, depression, or trauma may impair judgment and increase risk-taking online.

- 1:1 Teaching: Requires clear boundaries and safeguarding protocols to prevent inappropriate contact or misunderstandings.
- Reduced Supervision: Students may access unfiltered content or engage in risky behaviour without adult oversight.

3.2 Online Threats
- Cyberbullying
- Grooming and Exploitation
- Radicalisation
- Misinformation and Disinformation
- Sextortion and Image-Based Abuse
- Online Gaming Risks
- Digital Addiction

4. Online Safety Risk Assessment – BHES

Risk	Description	RAG Rating	Actions to Reduce Risk
Online Grooming	Vulnerable students may be targeted by predators via social media, gaming, or messaging apps.	Red	Educate students on grooming signs; Use filtered devices; Monitor online activity; Staff training; Encourage open communication
Radicalisation	Students may be exposed to extremist ideologies online, especially when isolated.	Red	Prevent training for staff; Monitor online content; Promote critical thinking; Report concerns to Prevent team
Cyberbullying	Students may be bullied via social media or messaging platforms.	Amber	Embed anti-bullying education; Encourage reporting; Monitor school devices; Support victims
Exposure to Inappropriate Content	Students may access violent, sexual, or harmful content.	Red	Use web filtering; Educate on safe browsing; Supervise sessions; Provide parental guidance
Sextortion / Image-Based Abuse	Students may be coerced into sharing explicit images.	Red	Teach about consent; Promote reporting; Involve police; Support victims

Digital Addiction / Overuse	Excessive screen time may affect wellbeing and learning.	Amber	Promote screen breaks; Balance online/offline learning; Educate on healthy tech use
Misinformation / Disinformation	Students may believe or share false information.	Amber	Teach digital literacy; Encourage fact-checking; Discuss current events
Inappropriate Staff-Student Contact	Risk of boundary breaches in 1:1 online or home settings.	Red	Use approved platforms; Record sessions; No personal accounts; DSL oversight
Lack of Parental Oversight	Parents may not monitor or understand online risks.	Amber	Provide training/resources; Share updates; Encourage parental controls
Data Privacy Breaches	Risk of personal data being shared or accessed inappropriately.	Amber	Use secure platforms; Train staff on GDPR; Limit data sharing; Conduct audits

5. Safeguarding Measures

5.1 Staff Protocols
- All 1:1 online sessions must be conducted via approved platforms with recording or logging enabled.
- Staff must never use personal devices or accounts to contact students.
- Two adults should be aware of all 1:1 sessions; DSLs must be informed of any concerns.
- Staff receive annual training on online safety, including updates on emerging threats.

5.2 Student Education
- Online safety is embedded in the PSHE curriculum and revisited regularly.
- Topics include: privacy settings, healthy online relationships, recognising grooming, and reporting abuse.
- Students are encouraged to critically evaluate online content and understand digital footprints.

5.3 Parental Engagement
- Parents/carers receive guidance on:
  - Setting parental controls

- Monitoring screen time
  - Recognising signs of online harm
- BHES hosts termly online safety workshops and shares updates via newsletters.

5.4 Technical Controls
- All BHES devices are equipped with:
  - Web filtering
  - Monitoring software
  - Antivirus and firewall protection
- Students using personal devices are supported to install appropriate safeguards.

6. Support and Reporting Pathways

6.1 For Students
- Talk to a trusted adult – your teacher, tutor, or a parent/carer.
- Contact the BHES Designated Safeguarding Lead (DSL)
- CEOP: https://www.ceop.police.uk
- Childline: Call 0800 1111 or visit https://www.childline.org.uk

6.2 For Parents and Carers
- Speak to your child's BHES teacher or the DSL
- NSPCC: Call 0808 800 5002 or visit https://www.nspcc.org.uk
- Internet Matters: https://www.internetmatters.org
- UK Safer Internet Centre: https://www.saferinternet.org.uk

6.3 For Staff
- Report immediately to the DSL or Deputy DSL
- Log the concern on the school's safeguarding system (CPOMS)
- Access training and resources via:
  - UK Safer Internet Centre
  - National College / Educare
  - Prevent Duty Guidance

7. Roles and Responsibilities

Role	Responsibility
DSL	Lead on safeguarding and online safety
Online Safety Lead	Monitors trends, updates policy, delivers training
Teaching Staff	Embed online safety in teaching, report concerns

Parents/Carers	Support safe use of technology at home
Students	Engage with online safety education and report issues

8. Policy Review

This policy is reviewed annually or in response to:

- Significant incidents
- Changes in legislation or guidance
- Emerging risks or technologies